Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Acceptable Use**
Number:	**ITP-BW-01**
Publish date:	**May 16, 2019**

1.0 Overview

Baldwin Wallace University is hereinafter referred to as "BW".

Though there are a number of reasons to provide a user access to BW IT resources, by far the most common is granting access to students for educational/research purposes or employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the BW IT resources. This policy explains how BW Information Technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using BW IT resources. Questions on what constitutes acceptable use should be directed to the HelpDesk, faculty advisor or if an employee, the user's supervisor.

2.0 Purpose

Information Technology, and other University departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Additionally, inappropriate use of BW systems can expose BW to legal, financial or other types of risk. Therefore, it is important to specify what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of BW Information Technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of BW information resources, owned, managed or provided by BW. These IT resources include, but are not limited to, computer systems, cloud services, email, the network, and the BW Internet connection.

Also included are personally-owned devices, including student and contractor devices, that are attached to a BW network.

4.0 Policies

4.1 Network Access

As the user will be given access to the BW network, Internet, and other IT resources, BW expects the user to use these resources in a responsible manner.

The user must make a concerted effort to avoid accessing network data, files, and information that are not directly related to his or her job function if employed by BW or role as a student attending BW. Existence of access capabilities does not imply permission to use this access.

4.2 Web Browsing and Internet Usage

The Internet is a network of interconnected computers of which BW has very little control. The user must recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate, or that may be illegal in some jurisdictions. The user must use the Internet at his or her own risk. BW is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

4.2.1. Personal Use

BW recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of BW computer systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on BW operations or on the user's job performance.

4.2.2 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) file sharing/networking applications (examples include but are not limited to: Ares Galaxy, Vuze, Limeware, uTorrent, BitTorrent, eMule, Shareaza, Frostwire) are not allowed on the BW business network under any circumstance. Students may use this technology on the student network provided by BW so long as it does not violate any other part of this policy such as prohibiting illegal activities.

4.2.3 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Reasonable use of streaming media for research or educational purposes is permitted on both the student and business network as long as it does not negatively impact the computer network or, if employed by BW, the user's job performance.

4.2.4 Blogging

Blogging by BW's employees is subject to the terms of this policy, whether performed from the BW network, personal systems, or other external systems. The user is asked to recognize that information posted on a blog immediately becomes public information and thus to exercise extreme discretion in the type of information posted. In no blog or website, including blogs or sites published from personal or public systems, shall internal BW business matters be discussed, confidential or sensitive data released, or material detrimental to BW published. See the “Community Standards of Conduct” for additional guidance.

As long as BW policies, as specified herein, are followed, BW allows the publishing and use of blogs. However, when done from the BW network or during business hours, blogging by employees of BW must either A) be business related, or B) consume no more than a trivial amount of the user’s time and network resources. The user assumes all risks associated with blogging.

4.2.5 Messaging

The user should recognize that messaging technologies, such as and not limited to email, instant messaging, social media platforms, and SMS (text) messages, unless specific encryption measures are taken, are not considered secure methods of communication. The user must follow all policies to prevent the disclosure of confidential data, specifically that unencrypted confidential data, such as Credit Card Primary Account (PANs), student data or other sensitive data as defined by the Data Classification Policy must never be sent via messaging technologies in an unencrypted form.

4.2.6 Bandwidth Usage

Network bandwidth is a shared resource that must be used as such. Excessive use of BW bandwidth or other computer resources, where not required by job function or role as a student, is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low BW-wide usage. Students in the Residence halls may not monopolize internet bandwidth resources. Examples of this include but are not limited to streaming services or gaming applications that generate an obsessive amount of network traffic. BW may restrict bandwidth for certain services deemed non-critical to BW operations, or as it sees fit to preserve network functionality.

4.2.7 Social Networking/Social Media

Social networking creates risks for BW in two ways: 1) in the potential sharing of BW confidential, private, or embarrassing information, and 2) the potential for an attacker to use posted information to craft a social engineering attack on BW. The user is asked to recognize that information posted on social networking sites is public information and to exercise extreme discretion in the type of information posted. No confidential information or sensitive is to be posted on social networking sites. Further, the user should restrict his or her privacy settings to fullest extent possible. The user must not publish any information detrimental to BW, its students, or employees that would cause embarrassment to BW on social networking sites.

As long as BW policies, as specified herein, are followed, BW allows reasonable use of social networking sites from its network and/or during business hours. This use must either A) be business related, or B) consume no more than a trivial amount of the user's time and network resources. The user assumes all risks associated with social networking.

4.3 Unacceptable Use

The following actions shall constitute unacceptable use of the BW network. This section is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable.

4.3.1 Prohibited Actions

The user may not use the BW network and/or systems to actions such as but not limited to:

- Engage in activity that is illegal under local, state, federal, or international law (see section "Use for Illegal Activities" for more information)
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to BW.
- Download, store, or distribute violent, perverse, obscene, lewd, or offensive material
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media
- Engage in activities that cause an invasion of privacy
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace
- Make fraudulent offers for products or services
- Reveal personal or network usernames or passwords to others, including family, friends, or other members of the household when working from home or remote locations
- Any unauthorized attempt to modify computer equipment or peripherals owned by BW
- Any unauthorized attempt to add, delete, or modify, or duplicate copyrighted software (such as operating systems, compilers, utility routines, graphics, games, etc.) owned by BW
- Attempted or actual use of accounts, files, or passwords without authorization from the owner
- Reading, copying, modifying, or deleting private files (including those belonging to any students, faculty, staff, or the University's administrative or academic files) without proper authorization

- Use the University's network to communicate messages to others that are harassing, offensive, or obscene
- Attempt to crash the BW servers, intranet, or public electronic networks
- Violate intellectual property rights or copyrights in data or programs
- Destruction, damage, or theft of equipment, software, or data belonging to BW
- Give unauthorized persons access to BW facilities by divulging passwords
- Establish an individual wireless network on campus or connecting any device (other than a computer) to the network without authorization from the IT Department

4.3.2 Circumvention of Security

Using any computer systems to attempt circumventing any security systems, authentication systems, user-based systems, or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent BW security systems is expressly prohibited. This includes disabling or tampering with any security software, such as antivirus/anti-malware software or remote access software.

4.3.3 Use for Illegal Activities

No computer systems or devices shall be used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking, including: packet sniffing, port scanning, packet spoofing, denial of service, wireless hacking
- Attempts to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Cybercrime, extortion, or Identity Theft
- Downloading, storing, or distributing any material prohibited by law
- Downloading, installing, or distributing unlicensed or "pirated" software
- Sending unsolicited bulk email or other messages deemed illegal under applicable regulations.
- Any other activity that circumvents the intended use of the system and or impacts the integrity of the University Networks and Systems

BW will take all necessary steps to report and prosecute any violations of this policy.

4.3.4 Overuse

Actions detrimental to the computer network or other BW resources, or that negatively affect student and/or employee job performance, or BW operations are not permitted. The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources are used appropriately.

4.3.5 Copyright Infringement

BW's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the Acceptable Use Policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using any method, unlicensed websites, or unlicensed media; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above. For additional guidance see BW Intellectual Property Policies in the BW Employee Handbook.

4.4 Monitoring and Privacy

Users should expect no privacy when using the BW network or BW resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. BW reserves the right to monitor any and all use of the computer network. To ensure compliance with BW policies this may include the interception and review of any emails, or other messages sent or received; inspection of data stored on personal file directories, hard disks, and removable media; and monitoring of Internet/network usage.

4.5 Responsible Computer and Network Use

BW expects users to use the network responsibly. Personal usage of BW computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on BW operations or on the user's job performance.

4.5.1 Non-BW-Owned Equipment

4.5.1.1 Non-BW-Owned Equipment Permitted

User or contractor provided computer equipment and devices (other than prohibited in section 4.5.1.2) are generally permitted to connect to BW's network shall adhere to Acceptable Use Policy and all other IT Policies and Standards. Examples of these devices are: laptops, notebooks, tablet computers, smartphones, game consoles/devices, etc.

4.5.1.2 Non-BW-Owned Equipment Prohibited

Non-BW-provided computer equipment that are prohibited for use at BW include:

- Any form of network device used for routing traffic such as, but not limited to: hubs, repeaters, gateways, wifi router, firewalls, …
- To protect the privacy and confidentiality of material being worked on by members of the BW workforce, any device that has the ability to continuously listen to conversations such as personal virtual assistants. (Examples: Amazon Alexa, Google Assistant or other such devices.)

4.5.2 Removable Media

In an open environment such as higher education, the use of personal storage devices is common but represents a very serious threat to data security. Examples of this devices are: USB drives, flash storage, media players, etc.

When using removable media, all rules for handling confidential data, such as those defined in the Data Classification Policy, must be strictly followed. This includes the use of encryption technologies to protect the information stored on these devices in case they are lost, stolen or access inadvertently obtained. For more information on proper encryption please visit http://help.bw.edu

4.5.3 Software Installation

Unauthorized installation of non-BW-supplied software applications on BW resources is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

4.6 Reporting of an IT Security Incident

See something say something! It is critical that users immediately report any suspicious activity so the university can quickly mitigate security threats. If an IT security incident or breach of any security policies

is discovered or suspected, the user (student, employee, or contractor) must immediately notify the BW Help Desk. Examples of incidents that require notification include but not limited to:

- Suspected compromise of login credentials (username, password, etc.)
- Suspected virus/malware/Trojan infection
- Loss or theft of any device that contains BW information
- Loss or theft of ID badge, keycard, or two-factor authentication token
- Any attempt by any person to obtain a user's password over the telephone or by email
- Any other suspicious event that may impact BW's information security.

4.7 Applicability of Other Policies

This document is part of BW's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

5.1 Employee Enforcement

This policy will be enforced by the Chief Information Security Officer, Chief Information Officer, and BW Administration. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.

5.2 Student Enforcement

Suspected misuse of the facilities should be reported to the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). The CISO and/or CIO, who is authorized to determine if there has been a violation of policy or law will refer student violators to the Office of Student Conduct for resolution. Pending the outcome, access to the shared technology resources may immediately be restricted or suspended. In some cases, limited access will be provided to the facilities needed for University-related activities, such as classes. Violations can result anywhere from Conduct Probation to suspension or expulsion from the University. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.